# システムのセキュリティ評価技術に関する研究開発

難波 電　金子 浩之　原 慎一郎　加藤 周　宇賀村 直紀

社団法人電子情報技術産業協会（JEITA）

ISO国際標準であるセキュリティ評価基準CC（Common Criteria for Information Technology Security）に基づくセキュリティ評価は、日本の制度上、セキュリティ評価技法CEM（Common Methodology for Information Technology Security Evaluation）に従い行うことになっているが、現状のCEMは主として単体のIT製品のセキュリティ評価を想定していると考えられ、ITシステムのセキュリティ評価向けには不十分なものである。実際、ISO/IECにおいてセキュリティ評価技法に関する標準化が検討されているが、運用システムに対する具体的な評価技法は検討の緒についたばかりである。このような課題を背景に昨年度の研究開発では、EC（Electronic Commerce）関連の実運用を想定したシステムをモデルにして、CEMをベースにシステム評価における留意点や解釈の仕方を抽出し、開発したシステム評価技法により試行評価を行い、欧米の評価機関による検証も実施した。本年度の研究開発では、昨年度開発したシステム評価技法に基づき、システム評価技法の方法論や証拠資材作成の指針を洗練しつつ、電子政府関連の実運用システムを対象にして、正式な評価を受けるためのシステム評価用証拠資材一式の作成を行った。また、「セキュリティ設計評価支援ツール」の改善を行った。

## 1.　はじめに

政府は、行政の効率化や国民負担の軽減を目標に、行政手続きを電子化する電子政府の基盤を2003年度までに構築することを目指している。

電子政府の構築は、デジタル経済・社会の一つのモデルである。その中で実施される情報セキュリティ確保のための対策もまた、広く民間の範となるべきものであり、これによって、我が国の情報システム全体の安全性・信頼性が高まり、更に、国際的な信頼性の確保につながることも期待される。このため、電子政府の構築に向けて、情報セキュリティ政策を重要なものとして位置づけ、積極的に推進していく必要がある。

本研究開発は、電子政府の推進において情報セキュリティ面がネックとならないよう、電子政府における信頼できる情報セキュリティ確保のための基盤技術の開発を行うことを目的として、情報処理振興事業協会からの委託により実施するものであり、平成13年4月からスタートした「情報セキュリティ評価・認証体制」を運営していく上での中核技術に関わるものである。

ISO国際標準（ISO/IEC 15408）であるセキュリティ評価基準CCは、平成12年7月にJIS X 5070としてJIS化もされているが、内容的にはIT製品やITシステムに、想定される脅威に応じた十分なセキュリティ機能が作り込まれ、運用可能であることを保証するためのものである。欧米では10年以上前から、このようなセキュリティ

評価技術の重要性が認識され、標準化が進み、国ごとの評価・認証制度が運用されてきており、現在では CC に基づく国際間の相互承認協定にまで発展している。しかしながら、それら先進各国においても、セキュリティ評価は未だ IT 製品単体に対するものが中心であり、運用される IT システム（以下、システムと呼ぶ。CC でいう「システム評価」とは、特定の目的と運用環境を持った IT システム全体を評価対象とするものである）を対象にするセキュリティ評価技術は開発段階である。日本においても、今後電子政府をはじめ、ネットワーク化を要とした電子化が進展すると予想され、種々構築されるシステムに対するセキュリティ評価は重要であり、ニーズが高いと予想される。

CC に基づくセキュリティ評価は、日本の制度上、セキュリティ評価技法 CEM に従い行なうことになっているが、現状の CEM は主として単体の IT 製品のセキュリティ評価を想定して作成されていると考えられ、システム評価向けとしては不十分であり、システム評価としての解釈の仕方や評価方法論自体を検討する必要があると考えられる。

また、現状の CEM の発想をそのままシステム評価に適用すると、単体評価に比べて評価作業がはるかに複雑になり、開発者や調達者に多大の負担をかける恐れがある。一つのシステムの評価に一年あるいはそれ以上の時間がかかったりすると実用上、大きな問題であると考えられる。

これらの課題に対処するには、実用上十分なセキュリティ評価レベルを保ち、かつ開発者や調達者が許容できる範囲内でセキュリティ評価を実施できる、システムを対象とした新しいセキュリティ評価技術の開発が必要である。

社団法人電子情報技術産業協会（以下、JEITA と呼ぶ）では、このような新しいセキュリティ評価技術を目指し、平成 12 年度に情報処理振興事業協会からの委託により、実運用される EC 関連のモデルシステムに基づいてシステムセキュリティ評価技法（以下、システム評価技法と呼ぶ）の開発を行い、欧米の評価機関による検証も実施した。

## ２．　研究開発の目標と内容

本研究開発の目標は、平成 12 年度に開発したシステム評価技法を、電子政府関連の実運用システムに適用し、開発面から、その実用性、有効性、負荷などについての検証を行うことである。

平成 12 年度に開発したシステム評価技法では、システムとしての特徴的なセキュリティ問題を具体化しつつ実効性が少ない評価項目を削減し、システムに適用できる実用的な評価技法の開発を目指していた。また、本システム評価技法は、開発作業に影響を与えるものであることもいうまでもないが、多大な負荷を課するものであれば、本評価技法自身が実用性のない、意味を持たないものになってしまう。

本研究開発では、具体的には、電子政府関連の実運用システムを対象に、本システム評価技法に基づくシステム評価を実施するために必要な種々の証拠資材（エビデンス）を作成することを通して、特に、開発者にとっての実効性（実現性、有効性、所要時間等）について検証を行う。また、作成した証拠資材は、来年度の研究開発として予定している当該システムの正式な評価機関による評価において、使用されるものである。

また、平成 12 年度に開発を行ったセキュリティ設計評価支援ツールの機能拡充及び適用拡大を目的とした改良を行う。まず、システム評価向けにセキュリティ評価文書管理機能を充実させる。加えて、Oracle8i Personal Edition 以外にフリーDB 一種をサポートするように、ツールのサポート DB の種類を拡大する。これらの改良によって、今後のシステム評価への適用拡大及び、セキュリティ評価技術の普及促進がより一層期待される。

## ３．本年度の活動状況

### ３．１ 評価対象のシステム

本年度の研究開発を実施するための対象として、電子政府関連の実運用システムである某社開発の電子申請システムを採用した。

電子申請システムを CC に基づき評価する上での

評価対象範囲である TOE（Target Of Evaluation）を、以下の図 1 に示す。

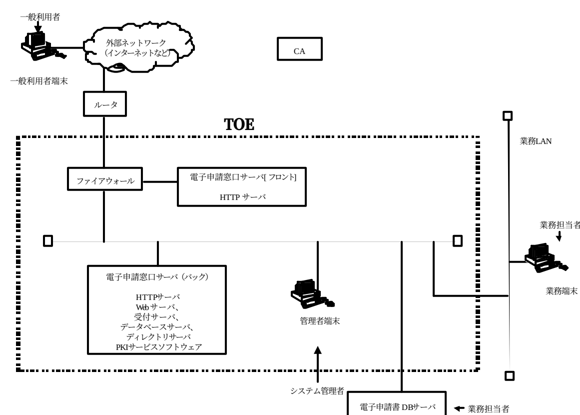



図１．評価対象の電子申請システム

### ３．２ システム評価用証拠資材の作成

電子申請システムを CC に基づき評価することを想定し、EAL3+（EAL3 追加）認証取得を目指し、正式な評価用証拠資材（以下、証拠資材と呼ぶ）一式の作成を行った。証拠資材の作成は、上記システムの開発者と共同で分担して行なった。

証拠資材の作成は、下記の手順で行なった。

（1） システム評価としての TOE の決定

電子申請システムのどの範囲を TOE にするかをシステム評価の特性を考慮しつつ、開発者と共同で検討し、決定した（図１参照)。

（2） 認証取得レベルの設定

認証取得を目指す評価保証レベルとして、昨年度の成果のひとつである電子政府 PP（電子申請システム PP 等）作成時の考察などを参考に、開発者の合意のもと EAL3+(追加の具体的内容については下記（3）参照）を設定した。

（3） システム評価技法の説明

電子申請システムの TOE に関して、EAL3+認証取得のための証拠資材を作成するために、昨年度開発したシステム評価技法を見直しつつ、開発者へのコンサルテーションとして見直し版の説明を行なった。

説明した項目は下記のとおりである。

● 開発（ADV クラス）

ADV_FSP.1（非形式的機能仕様)、ADV_HLD.2（セキュリティ実施上位レベル設計)、ADV_RCR.1(非形式的対応の実証)、ADV_SPM.1（追加）(非形式的な TOE セキュリティ方針モデル）

● テスト（ATE クラス）

ATE_COV.2（カバレージの分析)、ATE_DPT.1(テスト：上位レベル設計)、ATE_FUN.１（機能テスト)、ATE_IND.2（独立テスト - サンプル）

● ガイダンス（AGD クラス）

AGD_ADM.1（管理者ガイダンス)、AGD_USR.1（利用者ガイダンス）

● 構成管理（ACM クラス）

ACM_SCP.1（TOE の CM 範囲)、ACM_CAP.4（追加）(生成の支援と受入手続き）(ただし、EAL.3に ACM_CAP. ３はあり）

● ライフサイクルサポート（ALC クラス）

ALC_DVS.1（セキュリティ手段の識別)、ALC_LCD.1（追加）(開発者によるライフサイクルモデルの定義)、ALC_FLR.1（追加）(基本的な欠陥修正）

● 配布と運用（ADO クラス）

ADO_IGS.1（設置、生成、及び立ち上げ手順)、ADO_DEL.1（配付手続き）

● 脆弱性分析（AVA クラス）

AVA_SOF.1（TOE セキュリティ機能強度評価)、AVA_MSU.1（ガイダンスの検査)、VLA.2（追加）(独立脆弱性分析）(ただし、EAL.3に AVA_VLA.1はあり）

（4） 証拠資材の作成

証拠資材の作成は、開発者と共同で行なった。作成過程においては、作成指針を共同で検討し、また、開発者の作成物に対して種々コメントを行い、証拠資材の洗練を図った。

### ３．３ セキュリティ設計評価支援ツールの改善

セキュリティ評価文書管理機能を充実させることにより、システム評価向け使用に耐える回答を導きだせることを目的として、質問事項および回答のための手引き機能の改良を実施した。あわせて、これらツールの利便性を高めるために、従来、有償ソフトウェアを利用していた形態を、無償ソフトウェアでも利用できるように変更した。

### ３．４ 活動スケジュール（概要）

| 活動内容 | 予定スケジュール |
|---|---|
| ST 作成 | 9 月～10 月：一通り作成<br>2 月まで：調整、修正 |
| 開発仕様書類作成 | 9 月～1 月：可能なものから順次作成<br>2 月：調整、修正 |
| テスト | 12 月～2 月初旬：実施 |
| 開発者向けガイダンス | 9 月～1 月：情報収集<br>12 月～2 月：作成 |
| ツール改善 | 9 月～11 月中旬：設計<br>11 月中旬～2 月：開発・テスト |

### ３．５ 活動の成果

（１） 成果一覧

本研究開発のアウトプットを以下に列挙する。

＜システム評価用証拠資材一式＞

| 保証クラス | 証拠資材 |
|---|---|
| ASE | ・ST |
| ADV | ・機能仕様書<br>・構成仕様書<br>・セキュリティ方針モデル分析書 |
| ATE | ・機能テスト仕様書<br>・機能テスト結果報告書 |
| AGD | ・ガイダンス文書 |
| ACM | ・構成管理関連文書 |
| ALC | ・ライフサポート関連文書 |
| ADO | ・配布及び運用関連文書 |
| AVA | ・脆弱性分析書<br>・侵入テスト仕様書<br>・侵入テスト結果報告書<br>・TOE セキュリティ強度分析書 |

＜開発者向けガイダンス＞

上記システム評価用証拠資材作成の過程から得た知見等を､「開発者向けガイダンス」としてまとめた。

＜セキュリティ設計評価支援ツール改善関連＞

・フリーDB 使用調査報告書
・ソースプログラム
・オブジェクトモジュール
・基本設計書
・構成仕様書
・試験仕様書
・利用者マニュアル
・インストール説明書
・取扱説明書

（２）証拠資材作成の指針・課題と作成から得た知見

証拠資材作成においては、昨年度開発したシステム評価技法を見直し、証拠資材作成の指針、および明確でない点については課題として提示し、作成を進めた。作成過程における検討から、種々の知見等を得ることができた。

以下に各保証クラスごとの作成指針・課題と作成過程から得た知見等について、主な点の概要を示す。

① ASE

【作成の指針・課題】

● TOE の設定の仕方

１．に記述したように、CC でいうシステム評価とは、実運用されるシステム全体を評価対象とするものであり、当該システムの主目的とするアプリケーションのみならず､そのベースとなる OS､DBMS 等や補助的な FW 等もすべて TOE に入れる必要がある。また、システム評価の TOE は、基本的に業務のまとまりを範囲とすべきであり､TOE に入れない要素については、管理主体が異なるなど正当な理由が必要である。

● TOE の記述の仕方

システムの場合、複数の COTS などを設定して使用している場合が多いと思われるが、その設定、運用、管理を行うためのインタフェースを考慮して機能を記述する必要がある。

● 脅威分析

脅威分析では、どのようにして漏れなく脅威を洗い出すかが課題である。

【獲得した知見等】

● TOE の設定及び記述

上記の指針に基づき、TOE の設定（図１参照)、及び記述を行った。

● 脅威分析

「保護対象資産」と「脅威の手段と影響」による

マトリクスを作成し、そのすべての升目に前提（何らかの脅威に対抗するはず）または脅威の識別子を埋めていくことにより、脅威の網羅性を示すことができる。

その場合、「脅威の手段と影響」の網羅性が問題となる。特に、システム評価の場合、保護対象資産があちこちにフローするため、保護対象資産の存在する場所に注目して手段と影響を分類していくことで手段と影響はかなり整理され、網羅性は十分なものになると考えられる。脆弱性分析においてより詳細な、突っ込んだ分析を行う。

② ADV

【作成の指針・課題】

● 機能仕様

基本的には、評価対象システムの主目的である電子申請アプリケーションのみならず、その基盤をなす OS、DBMS 等や補助的に使われる FW 等、TOE を形成するすべてのソフトウェアのセキュリティ機能、およびそれらのセキュリティ機能を使うためのすべての外部インターフェースを記述する必要がある。

● 上位レベル設計

現状の CEM では、TOE をサブシステムに分けサブシステム間のインターフェースをすべて記述する必要があるが、COTS 間のインタフェースはわからないこともある。どのように考えるべきか。また、サブシステムへの切り分け自体、意味のあるように考える必要がある。

● セキュリティ方針モデル

ST4 章に対応して ST5 章で記述される機能要件では、FDP_ACF、FDP_IFF を除き背後にあるセキュリティ方針（TSP）が明確に記述されないため、ST（5 章－＞6 章－＞8 章）から機能仕様書へというブレークダウンにおいて、各機能要件の背後にある TSP が確実に実装されているかどうかが必ずしも明確ではない。特に、システム評価においては TOE 内のセキュリティ機能が多量で複雑であり、また、同一の機能要件が繰り返され（iteration）、同様なセキュリティ機能が TOE 内に広がり、散在する（例.監査機能が TOE 内の複数箇所のサーバの複数のソフトウェアに装備されている）ことがよくあるため、セキュリティ方針モデル（安全な状態遷移を示す特性と規則からなるモデル）を作成し、全体として TSP が実現されていることを確実に検証することが大事であると考えられる。

【獲得した知見等】

● インタフェースの捉え方

機能仕様で考えるべき外部インタフェース、及び上位レベル設計で考えるべきサブシステム間インタフェースについて、下記のように捉えることができる。

TOE の運用において利用されないインタフェースは、大まかに識別しておけばよく、インタフェースの説明は特に不要である。それで CC の要件は満足される。ただし、インタフェースが悪用できない状態になっていることの説明は必要である。

信頼できる利用者や COTS だけが利用するインタフェースについても、同様に細かい識別や説明は不要であると考える。大まかな識別だけ行って、確かに信頼できる利用者や COTS だけが利用できることが説明されていれば、そのインタフェースは悪用されないということになるため、TOE のセキュリティの観点からは十分であるといえる。ただし、そのようにした場合、CC の要件が厳密には満たされない可能性があり、今後の検討課題といえる。また、COTS を無条件で信頼してよいかどうかについても検討の余地がある。

信頼できない利用者に利用される可能性のあるインタフェースは、CC の要件通りにすべて識別して記述し、悪用できないことを検証しなければならない。ただし、信頼できない利用者に利用可能な状態で開放されるインタフェースを必要最小限にすることの方が重要である。

● サブシステムの定義

上記のようにインタフェースを扱えば、サブシステムを、COTS または数個の COTS を組み合わせたものとして定義し、意味のある評価が行えると考えられる。

● 開発過程とセキュリティ方針モデル

ST5 章や機能仕様書の作成において、セキュリ

ティ方針モデルに相当する内容は実質的に結構考えられていると思われる。ただし、意識的に一貫性を持って、無矛盾に考えられているかどうかは保証の限りではないので、セキュリティ方針モデルを作成し、検証することは重要であると考えられる。基本的に情報は結構ある（顕在、潜在）はずなので、それらを吸い上げ証拠資料を作成すればよい。

③ ATE

【作成の指針・課題】

● システム評価におけるテストの再現性

システムの TOE は、運用時の環境条件の変化によるさまざまな設定変更や新たなセキュリティ問題への対処など、日常的なマイナーアップデートが継続的に行われることにより、開発者がテストした時点の TOE と、評価を行なう運用中の TOE は実質的に異なる。したがって、システム評価におけるテストの再現性の保証は、極めて困難である。

● TOE 内の COTS関連のテスト

製品をコンポーネントとして使用する場合、その製品が具備するセキュリティ機能をテストすることが困難なことがある（例.RAID の機能を試すための障害発生が困難。製品評価では、もちろんそのようなテスト実施は必須）。また、TOE の TSFI（TOE Security Function Interface）が製品のセキュリティ機能の振る舞いに関連する場合、テスト仕様を作成するための情報が不足することが多く、求められるレベルのテスト仕様の作成が困難であるとともに、証拠間の整合も取りにくくなる。

【獲得した知見等】

上記の課題はシステムに依存した特徴的なものと考えられるため、CC 評価技法側からのシステムへの適合が望まれる。たとえば、開発者によるテストの結果が正しいことは、開発者サイトで行なわれたテスト環境で確認し、現在の TOE の動作については、運用時の操作を検査し、ログ等で確認するなどの確認手順を明確化していつでも機能確認が行えるようにするなどの方策が考えられる。これとは別に、システム開発時の機能テストと各証拠との間で、実施時期やテストの観点の違い（通常の機能テストは業務よりの機能テストが主体となる）により、テストの深さや範囲の対応が取りにくくなる場合がある。これについては、ADV_FSP、ADV_HLD ファミリの証拠に記載すべき内容の検討を実際のシステム設計とともに行い、COTS の持つセキュリティ機能の外部インタフェースやサブシステム間インタフェースが確実にテストできるサブシステム分割とすることにより、これらの証拠間の整合上の問題を軽減できる。また、一般的な事項であるが、テストの目的、手法、手順、確認項目、期待される結果の記載が求められるため、記載事項を規定した各社のテスト基準が存在するなら、テスト基準そのものを CC に適合させることが効果的であると考えられる。

④ AGD

【作成の指針・課題】

基本的には製品評価の場合と同じであるが、システム評価の場合、特に留意すべき点として下記が挙げられる。

● システムの各利用者ごとの記述

システムの場合、利用者が製品に比べて多く想定されているのが一般的なので、各利用者（システム管理者、運用者、一般利用者等）ごとに、役割、責任、権限、操作、関連規定項目を記述する必要がある。

● 機能仕様書記載の外部インタフェースの記述

ガイダンスでは、システムの各利用者が利用できる TOE の外部インタフェースが識別されていなければならず、機能仕様書において適切に識別された外部インタフェースをガイダンス文書にももれなく記述する。

● COTS の特定の使い方

TOE に組み込まれている COTS 等の、TOE における特定の使い方を記述（既存ドキュメントの利用等）し、TOE に組み込まれているものの間の適切な連携を示す必要がある。

【獲得した知見等】

● 多岐にわたる運用管理の記述

システムの場合、運用管理上行うべきことが、定期運用作業、不定期運用作業、障害対応等多岐にわたるため、それらすべてについてガイダンス文書に記述する必要がある。

⑤　ACM

【作成の指針・課題】

●　運用中システムの構成管理

システム評価の場合、実運用システムが評価対象であるため、開発過程の構成管理だけでなく、運用中のシステムの構成管理までが評価対象になる。

●　構成管理の内容

運用中のシステムには、環境条件の変更にともなう設定変更、パッチ等による更新、データ領域の拡張など、運用方針及び計画に沿った構成要素の更新、構成の変更が日常的に発生する。また、開発、運用など関係する部門等が複数存在する場合が多いことが想定され、運用時に発生する構成変更とその維持管理に対して組織的な連携を要するとともに、運用タスクの複雑性が増す傾向にある。したがって、品質システムなどのインフラを整備し、実効力を高めるための継続的な見直しが求められる。

【獲得した知見等】

●　構成管理への対応の仕方

運用 TOE の構成管理を行うにあたり、ハードウェアやCOTSなど製品を活用しTOE用の設定を行って使用している部分、TOE のために独自に開発したプログラムコードやオブジェクトコードを管理する部分など、構成要素の特徴や目的別に適用する管理方法を分けることにより、実際のシステム運用に適した構成管理を行うことが可能と考える。具体的な例として、構成品目（ハードウェア、COTS ソフトウェア、マニュアル等）として管理する部分、TOE 独自の開発資産（独自開発プログラムコード、オブジェクト、TOE 生成ツール等）として管理する部分のそれぞれを管理する CM システムを構築し、前者は、構成リスト、設定リスト等により運用時の変更管理（台帳等を活用）を実施し、後者は本番環境、開発環境、及びこれらの環境間でやりとりする一時的な資源を管理する環境からなる CM システムで管理する。また、これら２つの CM システムを運用するための CM 計画を策定し文書化する。このように、特徴や目的別に複数の CM システムを運用し、これらを関連する複数の部門にまたがって組織的な連携のもとに維持管理することで、システムの特徴である複雑な構成管理を必要とする場合にも適合させることができると考える。

⑥　ALC

【作成の指針・課題】

●　システム評価における重要性

ライフサイクル定義、開発セキュリティ、欠陥修正は、システムに限らず重要な、開発者による組織的なマネジメントシステムを要求するものであり、システム固有の特徴的な課題等は見受けられない。ただし、実際に稼動するシステムでは、ALC クラスの保証要件はより重要なファクタであることから、確実に実施されるべき要件であると考える。

【獲得した知見等】

●　対応の仕方

ライフサイクル定義、開発セキュリティ、欠陥修正については、文書管理を含む所定レベルのマネジメントシステムを持つ開発者にとっては、要求事項へ対応するための微調整を行なうことで CC に適合させることができる場合が多い。CC で求めるレベルに達していないマネジメントシステムを持つ場合は、TOE 個別の管理手順を作成し適用することになる。構成管理、配付と運用など、運用系の CC 要件との関係は十分考慮する必要がある。

⑦　ADO

【作成の指針・課題】

●　配付関連

運用サイトでシステムを構築する場合と、開発サイトでテスト済みのシステムを運用サイトに持ち込む場合において、配付の形態が異なる。いずれの場合も本来の配付に係る保証要件を積極的に実施する必要性が製品にくらべて薄い傾向にあるが、コンポーネントである COTS 製品の配付については考慮すべきである。

●　設置、生成、及び立上げ

設置、生成、及び立上げは、システムの場合、複雑化の傾向にあるものの、各手順を明確に計画し、実施することにより、CC への対応が図れることから、規模により複雑性が増すこと以外のシステム固有の特徴的な課題等は見受けられない。

【獲得した知見等】

● 対応の仕方

意図的もしくは偶発的な改ざんを排除した適切なTOE のバージョンの配付を実現することは、技術的な対策よりはむしろ管理的な側面での補強がより有効である。組織的な配付手続きを決め、運用サイトで構築の場合は、構成要素が製品の配付手順にしたがって適切に配付し、設置、生成、及び立上げ手順によって適切に導入することにより、配付に起因するセキュリティ問題を排除することができると考える。なお、設置、生成、及び立上げ手順は、ST、ガイダンス、構成管理等との整合を踏まえ、綿密に計画されるべきであり、導入時に設定情報を記録し、これを運用にわたって維持することがシステム運用に際しては重要と考える。

⑧ AVA

【作成の指針・課題】

まず、脆弱性を漏れなく分析することが重要である。また、通常は COTS の内部の詳細な資料は入手できないが、その部分に関連する脆弱性をどう考えるかも課題といえる。

【獲得した知見等】

どの保護対象資産かよりも、資産の存在する場所に注目して分析を行う方が良い。脆弱性の分析は以下のように分類して行うと、煩雑になるのを防げる。

● TOE セキュリティ機能が正常動作の場合

TOE のセキュリティ機能が正常に動作した場合TOE のバグやセキュリティホールは悪用されないことを仮定すると、保護対象資産に対する脆弱性は発生しないことを検証する。保護対象資産が存在する場所から脅威エージェントまで逆方向にたどっていくのが、分析の網羅性という観点では良いと考えられる。

● TOE 自体の正常性の保障

TOE のバグやセキュリティホールは悪用されないことを仮定すると、TOE 自体の動作が保障されることを検証する。TOE を構成しているプログラムコードや TSF データなどに対する脆弱性が発生しないことを分析する。

● TOE のバグやセキュリティホールへの対応

TOE のバグやセキュリティホールが悪用されないことを検証する。一般に利用されている COTS については、また、システム向けに開発された部分でも、一般的なプロトコルやライブラリを利用している場合は、バグやセキュリティホールによる脆弱性が公知のものになりやすい。したがって、できるだけ最新のパッチを適用し、そのような脆弱性が残っていないことを検証する必要がある。脆弱性が残っていないことを検証するためには、十分な実績があり、セキュリティ情報の更新が絶えず行われているセキュリティ検査ツールを利用するのが妥当と考えられる。システム独自のプロトコルやロジックについては、バグやセキュリティホールが存在していても公知のものになりにくいので、開発者による脆弱性分析では考えなくてよいのではないかと思われる。

## ４．外部発表及び成果物

＜外部発表＞

本研究開発で得たものをベースに、ISO／IEC JTC1 SC27 のセキュリティ評価技法標準化プロジェクトに、システムの評価技法として提案を行なう予定である。

＜成果物＞（詳細は３．５（１）参照）

（１）システム評価用証拠資材一式

（２）開発者向けガイダンス

（３）セキュリティ設計評価支援ツール改善関連一式（プログラム、設計書等）

## ５．今後の課題

（１） 正式な評価の実施

今年度作成したシステム評価用証拠資材を基に来年度、電子申請システムの正式な評価機関による評価を実施する。

（２） システム評価技法の検証

来年度の正式な評価を通して、昨年度から今年度にかけて開発し、洗練したシステム評価技法の検証を行い、システム評価の見識（評価技法、評価方法論）を明確化する。

## ６．まとめ

電子政府関連の実運用システムである電子申請システムを対象に、昨年度開発したシステム評価技法を適用し、システム評価技法を洗練しつつ、正式な評価を受けるための証拠資材一式の作成を行なった。

その過程において、実現性、有効性、負荷等について有益な知見を得ることができた。

また、セキュリティ設計評価支援ツールのシステム評価向けの改善等を行なうことができた。

来年度は本年度の成果を基に、正式な評価機関による評価を実施し、その過程においてシステム評価技法の検証も行い、システム評価技法の確立を目指していく予定である。また、来年度以降、海外の評価機関による検証も実施する予定である。

## ７．参考文献


[1] 妹尾徹他：システムのセキュリティ評価技術に関する研究開発，IPA平成12年度電子政府情報セキュリティ技術開発事業年次総括報告書.

[2] Common Criteria for Information Technology Security Evaluation , Part1 ~ Part3, Version2.1, CCIMB, 1999.

[3] Common Methodology for Information Technology Security Evaluation，Part2, Version 1.0，CCIMB，1999.